採用Windows 7或Android VPN客戶端和證書身份 驗證配置的ASA IKEv2 RA VPN

目錄

 箇介

 必要條件

 需求

 採用元件

 設定

 概觀

 配置證書頒發機構

 生成客戶端證書

 在Windows 7客戶端電腦上安裝身份證書

 如何在Android流動裝置上安裝身份證書

 為使用IKEv2的RA VPN配置ASA頭端

 配置Windows 7內建客戶端

 配置Android本地VPN客戶端

 驗證

 疑難排解

簡介

本文檔介紹如何配置Cisco Adaptive Security Appliance(ASA)9.7.1版及更高版本,以便允許 Windows 7和Android本地(虛擬專用網路)VPN客戶端使用網際網路金鑰交換協定(IKEv2)和證書 作為身份驗證方法建立(遠端訪問)RA VPN連線。

作者:David Rivera和Cesar Lopez Zamarripa,思科TAC工程師。

必要條件

需求

思科建議您瞭解以下主題:

- 證書頒發機構(CA)
- 公開金鑰基礎架構 (PKI)
- ASA上帶IKEv2的RA VPN
- Windows 7內建VPN客戶端
- Android原生VPN客戶端

採用元件

本檔案中的資訊是根據以下軟體版本:

- CISCO1921/K9 15.5(3)M4a(作為IOS CA伺服器)
- ASA5506X 9.7(1)作為VPN頭端
- Windows 7作為客戶端電腦
- Galaxy J5 Android 6.0.1作為移動客戶端

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除(預設))的組態來啟動。如果您的網路運作中,請確保您瞭解任何指令可能造成的影響。

設定

概觀

以下是配置Windows 7和Android本地VPN客戶端以連線到ASA頭端的步驟:

配置證書頒發機構

CA允許將所需的擴充金鑰使用(EKU)嵌入憑證中。對於ASA頭端,需要證書伺服器身份驗證 EKU,而客戶端證書需要客戶端身份驗證EKU。

可以使用各種CA伺服器,例如:

- Cisco IOS CA伺服器
- OpenSSL CA伺服器
- Microsoft CA伺服器
- •3rd 參與方CA

此配置示例使用IOS CA伺服器。

本節概述使版本15.5(3)M4a的CISCO1921/K9作為CA伺服器工作的基本配置。

步驟1.確保裝置和版本支援eku命令。

IOS-CA# show run | section crypto pki
crypto pki server <CA_Server>
 issuer-name <cn=calo_root,ou=TAC,o=cisco>
 grant auto
 eku server-auth client-auth
步驟2.在路由器上啟用HTTP伺服器。

IOS-CA(config)#ip http server 步驟3.生成可匯出的RSA金鑰對。

IOS-CA(config)# crypto key generate rsa modulus 2048 label <HeadEnd> exportable
The name for the keys will be: HeadEnd
% The key modulus size is 2048 bits
% Generating 2048 bit RSA keys, keys will be exportable...
[OK] (elapsed time was 5 seconds)
步驟4.配置信任點。

IOS-CA(config)# crypto pki trustpoint <HeadEnd>

IOS-CA(ca-trustpoint)#enrollment url http://10.201.180.230:80
IOS-CA(ca-trustpoint)#subject-name <cn=HeadEnd.david.com>
IOS-CA(ca-trustpoint)#revocation-check none
IOS-CA(ca-trustpoint)#rsakeypair <HeadEnd>

附註:enrollment命令的IP地址是路由器為可達介面配置的IP地址之一。

步驟5.驗證信任點(取得CA憑證)。

IOS-CA(config)#**crypto pki authenticate** <HeadEnd> Certificate has the following attributes: Fingerprint MD5: DA4502F4 CEFB4F08 AAA3179B 70019185 Fingerprint SHA1: A887F6DB 0656C7E2 857749F3 EA3D7176 8920F52F % Do you accept this certificate? [yes/no]: **yes** Trustpoint CA certificate accepted. 步驟6.註冊信任點(獲取身份證書)。

IOS-CA(config)#crypto pki enroll <HeadEnd> 2 % Start certificate enrollment .. % Create a challenge password. You will need to verbally provide this password to the CA Administrator in order to revoke your certificate. For security reasons your password will not be saved in the configuration. Please make a note of it. Password: cisco123 Re-enter password: cisco123 % The subject name in the certificate will include: cn=HeadEnd.david.com % The subject name in the certificate will include: Connected_2_INET-B % Include the router serial number in the subject name? [yes/no]: no % Include an IP address in the subject name? [no]: no Request certificate from CA? [yes/no]: yes % Certificate request sent to Certificate Authority % The 'show crypto pki certificate verbose HeadEnd' command will show the fingerprint. *Jul 17 15:21:11.343: CRYPTO_PKI: Certificate Request Fingerprint MD5: 0017C310 9F6084E8 63053228 B449794F *Jul 17 15:21:11.343: CRYPTO_PKI: Certificate Request Fingerprint SHA1: CFE22C7A B2855C4D B4B2412B 57FC7106 1C5E7791 *Jul 17 15:21:15.675: %PKI-6-CERTRET: Certificate received from Certificate Authority 步驟7.驗證憑證。

IOS-CA#show crypto pki certificates verbose <HeadEnd> Certificate Status: Available Version: 3 Certificate Serial Number (hex): 05 Certificate Usage: General Purpose Issuer: cn=calo_root Subject: Name: Connected_2_INET-B hostname=Connected_2_INET-B cn=HeadEnd.david.com Validity Date: start date: 16:56:14 UTC Jul 16 2017 end date: 16:56:14 UTC Jul 16 2018 Subject Key Info: Public Key Algorithm: rsaEncryption RSA Public Key: (2048 bit)

Signature Algorithm: SHA1 with RSA Encryption Fingerprint MD5: 0017C310 9F6084E8 63053228 B449794F Fingerprint SHA1: CFE22C7A B2855C4D B4B2412B 57FC7106 1C5E7791 X509v3 extensions: X509v3 Key Usage: A0000000 Digital Signature Key Encipherment X509v3 Subject Key ID: E9B3A080 779A76E7 8BE44F38 C3E4DEDF 18E75009 X509v3 Authority Key ID: B5EEEEB9 31B9A06C CBD9893C 0E318810 5CA657E6 Authority Info Access: Extended Key Usage: Client Auth Server Auth Associated Trustpoints: HeadEnd Key Label: HeadEnd CA Certificate Status: Available Version: 3 Certificate Serial Number (hex): 01 Certificate Usage: Signature Issuer: cn=calo_root Subject: cn=calo_root Validity Date: start date: 13:24:35 UTC Jul 13 2017 end date: 13:24:35 UTC Jul 12 2020 Subject Key Info: Public Key Algorithm: rsaEncryption RSA Public Key: (1024 bit) Signature Algorithm: MD5 with RSA Encryption Fingerprint MD5: DA4502F4 CEFB4F08 AAA3179B 70019185 Fingerprint SHA1: A887F6DB 0656C7E2 857749F3 EA3D7176 8920F52F X509v3 extensions: X509v3 Key Usage: 8600000 Digital Signature Key Cert Sign CRL Signature X509v3 Subject Key ID: B5EEEEB9 31B9A06C CBD9893C 0E318810 5CA657E6 X509v3 Basic Constraints: CA: TRUE X509v3 Authority Key ID: B5EEEEB9 31B9A06C CBD9893C 0E318810 5CA657E6 Authority Info Access: Associated Trustpoints: test HeadEnd CA_Server 步驟8.將HeadEnd信任點匯出到PKCS12格式的終端以獲取身份證書。CA證書和私鑰新增到一個檔 案中。

IOS-CA(config)#crypto pki export

<ciscol23>

Exported pkcs12 follows:

MIIL3wIBAzCCC5kGCSqGSIb3DQEHAaCCC4oEgguGMIILgjCCC34GCSqGSIb3DQEH BqCCC28wggtrAgEAMIILZAYJKoZIhvcNAQcBMBsGCiqGSIb3DQEMAQMwDQQIocGz Fa6tZyACAQGAggs4qNTJi71/f0IvQr8n1c/SCeaSYRLBvcY9yPgJ2K2/Nmu9+KNB 3dAoYkCrGwDdfpobJE0XqBpIE1uBOtAeF7zdFJt/Pgpie4fcqpCVIbDXG8Ansmhj v0j6W9Z/IJHe7JrENatbi4nhTnCDP79Z65QSkzrb9DenkCGjoQsWP9zLHTiCDNzV ajMlWFuCFb0wSW/6L73BLTjS7rwtE74gYMU5NJwtOVsJM2LdwuQ+iOnpsnp6q9fu niUFEutPe8imOCRApe0tpPqhDp74hKziKT8JEsQ8HMO/lX1y/LIXdLISnz1nkoN3 vxD4AMGRFYACPH8PiGcVSx+vD+wmNaHp1vAOrq4pS7ZQ37ko4mFudnftdOUzaPIz EzTrOwlRE6il/gF8vb14EfeR09vumJBsajF12hrFGugIJTZnElp5go+oHEEAo4Y+ Yhoj/MIOyhZzo3/ujhjKqtsAJXybYF9YqVkTee9u4Xjkcsg5AmbaqeUUfd7Q8CC2 bi39S1maoWbTYiNcHFs/bWKWJsgZwPzfWtmPch/8MNvXn46AJAwIwRQjHruuFE9F bhv7SRhYSRQZPf7j1PTmJuMkKA3AzjdbmmJuLidbX3yKbTt4PxPMusbv+ojc6Nam RCsRf7+gnNZLWs3eU1n84rryZg5Pjw3MRTu2yXDvr799gvx7NIZH5yUZyV11T70b eC4KbflcmpM6mJ2UVnaoP2N5u892m41BWuk9rt5isl2f/Z/ZuSbkFaxzU0456zSq VbYsR+51XfQEH5xu88E5EUPWZ86YdUS1bD8ky6WOn0M104K6rNDLkqwXcxw3CaZ8 zhao+dE3qoEYWaKPgCQzPqW0BW3y7WSIELug2uSEsXQjIQcF+42CX6RA3yCmy2T8 C+osKlSSao0nzjrlpTWnPiFss9KRFgJDZhV2ItisiALNw9PqruddcmYtw44LXvdc +OfnyRvuLS6LE/AMmGk0GaVetAXPezD+5pVZW13UMT/ZdzUjLiXjV9GzF6V8i8qN Ua0MbDEa8T5Le4dCigaA+t1QxQ0PGb+w0ZAQzWN4gZpSEk3ejRixOt14SU5ivj/O lGXNn8Fvebk42CHohjXG9fq/IfbsVWSkxn2OZ/fhXkZztv4ic1VgprgJURjCtcBw 9Qp/ONda+9aDHiSBrKeHC/urgX6rgWXv9+hpRKIRfj3b8WE+N1sivuQEjlWxbD7h 9fpwxXb+/i7HisjzSkOWUNw4lyulfYSiOv86FPWK0H9Vjbg0G0di1rvGZ8uJHQCC 77RLFXp4jrvCgeo4oWKQbphgPAng7rT794vMwq0rYOb4D3HlHCUvU3JJmScDJQy2 zQxbG2q8Htm44COOuJEUBzx1ImayH2XvDck6VmLTGn8XH5Vq7L0lCeUcVDM8aQfy HJSPk/VmfQ01XwPIaxxYlr+jOpcorFkH+OH04hz07grAsGyLRoFICTEvHAzVnF0X 2A1j/z/BFAPG86ssAtInRZVeYUS72NwPEtpKmlHZnl+2iWno5iwTZqtjv7oREZKE RE6m708RiPSD2RjjamCmmmnH5dK5wxF7YlIeK/+ZVrfwLecEPRl+eVw0isM/JN/a WmkZkCcVMx/ec1P8jp8LzCx17HgVNYbg9lsiffD4xo0G/k0QLUlpliAt7LA2BeGs y155wtYUcOBH0/Es39yWnm2Ea//IK6BLw98PvU90vkXWwiD3ajFmcHmssDeU/tZR 4KKNuNor7Le9ycXZFM9ofKZ6AIJ9A1AYvOyhG088voq8MMGXEe/q+DIjaVE1htYu k0ELmYAD/X0kEvp3Sq0kLQZiCzZ20iMWUTWX1XfgrfLEH0utwHTyr3J2vQk5CD37 ZAfsF6zxEvtU2t41J0e90jWJw9WtWnnS0gzLeXWtW3H0YAIw3QodKNzbaY4eLP4y BEdsLmWbM4eza0m9BoZOmMUSkhvFrEz5Q5X5r9vCuAi1rYDqyIjhgdme56tVV0Vg ZauhbNX59PQQzwOdIZJVVL5tgjf0h7XCm90Bsqd121HurCCmHy7kM5pqf0MMlhH7 oM/DhXdTU+1sEabt/9c2qs1ihJLS1Zaw2q1AaS5h00+xL8Lxwh2/1/R7Q8FferhR QZDpix+CmtakRu7uPOMa0zsyOko3P9mf74AWDrThAwMA6G238TC6XI1vrXhvEX11 BVplQq0Wh/p7ZorSjD5l+z7TkXmJNp7iIxAqp0yobC6vOBwQP7/QAs88q9JNSAte ErdCXoizvs8YmZMoEap948oplYFaIP+xCnCr8l3v7znwfZwTMQPoPvqEFqUmWYgt xkJ0qaE645ihTnLgk4eg1sBLs1wPR1RJU+t6kGGAUmxqhPFxb3/1xNRPVzOGn12w S9yw+XLC6kS4PmKoxkxax4nnCx7s3e7B5e0qmYtgRTJ0GuW7Uf+T3royTOuYm0d+ ik6bmxcn00qdcHtt2HTbI+kYpken3YrF0h9Jnm9ZKT63gQSqQWL800ZVd4dAZceg FciNKs9r26fyy+L3rGCh+U9TLf6mNuWu8RstjjIGPHEPKZ9gnMgMJmikP2ghgOAd XVhs6ashXx33bZ9dIuhRx6uTNMrppsXyg6SxUyeGDYhpxsPt7uRwBswOpi6iDMZn ISSzQjrkxoNwwOfn8705fTCLhHlTZa8HS5HMK3KE7LiZv9pa1z6KTo4z+LCQSLDy FoRJhSaEsCYJsLDS5nYBoR8hE/eMvQDX1f+RZBrJDcftxx7FQ+8RtvHSJRcJK9N/ Ph/pL62NBlSbvCfnlAbisKrbbgCVLOSj/doufPvpMT2UDL0TY8UnQiyWMH1MF3tZ jJy6Si2glLwA9hu/c1NsREbA0gxMTjAREb5BjAUmlc3fuv2DWpwnkwyZNyHdm9B9 TPRoByGPvSZXa8MwY/8DUEwUQEsfDJi5jlAD416VFFUB72ZS7wn/mVR02fPkfOMp 3yhnGgX29OaDDiDlKw1Xwj1NybOhpZ6unDo5J3stMxlbv5TYL2Tl6egZS0SjsLmn cj5zkyUU22/93E5vfKD1CMiXx9/e4j2rRh3QCIXqaCjC9acTJ8a/k9/bp8Nz5Cir pnaCbuQsvna92nxVUqcmLlSbVIvGqlH9qm4DurhcLh59j20tX6K8AMJ90+azaYbX AJV/MCElhJg6wcN8QnCHMhiuK9+zpsUK2FQgfbcgaaNe3xGaXuoOIGQmlbAGtEkp kuauRzQ8/pwszaZuPh/5rE77z8zMut3+0E5CslB9npzNi0b0itaaRl13bBBml1xn r6SBUw7AWapZwRx6pihvptLJaqU1IzaV5SWk0zTABR7BmR84L0+/8v/bedcPSioG ecside21F6CcWO5ywABBxDYQXM1P9qkC/2bkPkEJ0jB15P5L1+Yqb8hTlone/InR B8ktEd8+QW8o60h0seONXumTqBfAuNBkprOA3ssXLeEGB01peC5oGW+VSziyS9id zYq8WaehpAIf3pqwn8gsi0B/wd57T0KK91+v0Ei4z+yIdu8Kh9GTiqGvgNAeakgr ECDiXoKAwltYAn7cLKNpZaojSs2Jt+60oBA5crT04Mtgpjb9Pd/DLqWQDJTyoRVv cJRb68a0yZvVBU0yoLbox84QKLHIsA92pplS7VFrAWP65wrhs4XOf4YSF1M89Sn4 GD/yEsGVJzwGrxgCNnOZkLIKsFbI0jp2lMps5jVKoFfpPJCie3F2FB3ecS+xRpHo 5u2KOTmH0rFQ6Vu+JYCo/qWh0ERtL/8gczP7C9ehiaZfemw2bq9xrUo+6y3H9Q+Z LADwMlAkI+kzbng3R+fj4AYBvf8GTJdpBs8s/t7mZXHiXCtH6qxTMRWJx5Xuxs9F I8Ii8TA9MCEwCQYFKw4DAhoFAAQUj0/On/REYODupznP9SwYnFX92BYEFESx1MSa ho3Cv1cZYM0TzZEzlsKdAgIEAA== ---End - This line not part of the pkcs12---

CRYPTO_PKI: Exported PKCS12 file successfully. *Jul 17 15:46:49.706: %PKI-6-PKCS12EXPORT_SUCCESS: PKCS #12 Successfully Exported. 步驟9.在ASA上建立空信任點。 ASA(config)# **crypto ca trustpoint** <HeadEnd> DRIVERAP(config-ca-trustpoint)# **exit**

ASA(config)#crypto ca import <HeadEnd> pkcs12 <cisco123>

步驟10 。匯入PKCS12檔案。

Enter the base 64 encoded pkcs12.

End with the word "quit" on a line by itself: MIIL3wIBAzCCC5kGCSqGSIb3DQEHAaCCC4oEgguGMIILgjCCC34GCSqGSIb3DQEH BqCCC28wggtrAgEAMIILZAYJKoZIhvcNAQcBMBsGCiqGSIb3DQEMAQMwDQQIocGz Fa6tZyACAQGAggs4qNTJi71/f0IvQr8n1c/SCeaSYRLBvcY9yPgJ2K2/Nmu9+KNB 3dAoYkCrGwDdfpobJE0XqBpIE1uBOtAeF7zdFJt/Pgpie4fcqpCVIbDXG8Ansmhj v0j6W9Z/IJHe7JrENatbi4nhTnCDP79Z65QSkzrb9DenkCGjoQsWP9zLHTiCDNzV ajMlWFuCFb0wSW/6L73BLTjS7rwtE74gYMU5NJwt0VsJM2LdwuQ+iOnpsnp6q9fu niUFEutPe8imOCRApe0tpPqhDp74hKziKT8JEsQ8HMO/lX1y/LIXdLISnz1nkoN3 vxD4AMGRFYACPH8PiGcVSx+vD+wmNaHp1vAOrq4pS7ZQ37ko4mFudnftdOUzaPIz EzTrOwlRE6il/gF8vb14EfeR09vumJBsajF12hrFGugIJTZnElp5go+oHEEAo4Y+ Yhoj/MIOyhZzo3/ujhjKqtsAJXybYF9YqVkTee9u4Xjkcsq5AmbaqeUUfd7Q8CC2 bi39S1maoWbTYiNcHFs/bWKWJsgZwPzfWtmPch/8MNvXn46AJAwIwRQjHruuFE9F bhv7SRhYSRQZPf7j1PTmJuMkKA3AzjdbmmJuLidbX3yKbTt4PxPMusbv+ojc6Nam RCsRf7+gnNZLWs3eU1n84rryZg5Pjw3MRTu2yXDvr799gvx7NIZH5yUZyV11T70b eC4KbflcmpM6mJ2UVnaoP2N5u892m41BWuk9rt5isl2f/Z/ZuSbkFaxzU0456zSq VbYsR+51XfQEH5xu88E5EUPWZ86YdUS1bD8ky6WOn0M104K6rNDLkgwXcxw3CaZ8 zhao+dE3qoEYWaKPgCQzPqW0BW3y7WSIELug2uSEsXQjIQcF+42CX6RA3yCmy2T8 C+osKlSSao0nzjrlpTWnPiFss9KRFgJDZhV2ItisiALNw9PqruddcmYtw44LXvdc +OfnyRvuLS6LE/AMmGk0GaVetAXPezD+5pVZW13UMT/ZdzUjLiXjV9GzF6V8i8qN Ua0MbDEa8T5Le4dCigaA+t1QxQ0PGb+w0ZAQzWN4gZpSEk3ejRixOt14SU5ivj/O lGXNn8Fvebk42CHohjXG9fq/IfbsVWSkxn2OZ/fhXkZztv4ic1VgprgJURjCtcBw 9Qp/ONda+9aDHiSBrKeHC/urqX6rqWXv9+hpRKIRfj3b8WE+N1sivuQEjlWxbD7h 9fpwxXb+/i7HisjzSkOWUNw4lyulfYSiOv86FPWK0H9Vjbg0G0di1rvGZ8uJHQCC 77RLFXp4jrvCgeo4oWKQbphgPAng7rT794vMwq0rYOb4D3HlHCUvU3JJmScDJQy2 zQxbG2q8Htm44COOuJEUBzx1ImayH2XvDck6VmLTGn8XH5Vq7L0lCeUcVDM8aQfy HJSPk/VmfQ0lXwPIaxxYlr+jOpcorFkH+OH04hz07grAsGyLRoFICTEvHAzVnF0X 2A1j/z/BFAPG86ssAtInRZVeYUS72NwPEtpKmlHZnl+2iWno5iwTZgtjv7oREZKE RE6m708RiPSD2RjjamCmmmnH5dK5wxF7YlleK/+ZVrfwLecEPRl+eVw0isM/JN/a WmkZkCcVMx/ec1P8jp8LzCx17HqVNYbq9lsiffD4xo0G/k0QLUlpliAt7LA2BeGs y155wtYUcOBH0/Es39yWnm2Ea//IK6BLw98PvU90vkXWwiD3ajFmcHmssDeU/tZR 4KKNuNor7Le9ycXZFM9ofKZ6AIJ9A1AYvOyhG088voq8MMGXEe/q+DIjaVE1htYu k0ELmYAD/XOkEvp3SqOkLQZiCzZ20iMWUTWX1XfgrfLEH0utwHTyr3J2vQk5CD37 ZAfsF6zxEvtU2t41J0e90jWJw9WtWnnS0qzLeXWtW3H0YAIw3QodKNzbaY4eLP4y BEdsLmWbM4eza0m9BoZOmMUSkhvFrEz5Q5X5r9vCuAi1rYDqyIjhgdme56tVV0Vg ZauhbNX59PQQzwOdIZJVVL5tgjf0h7XCm90Bsqd12lHurCCmHy7kM5pqf0MMlhH7 oM/DhXdTU+1sEabt/9c2qs1ihJLS1Zaw2q1AaS5h00+xL8Lxwh2/1/R7Q8FferhR QZDpix+CmtakRu7uPOMa0zsyOko3P9mf74AWDrThAwMA6G238TC6XI1vrXhvEX11 BVplQq0Wh/p7ZorSjD5l+z7TkXmJNp7iIxAqp0yobC6vOBwQP7/QAs88q9JNSAte ErdCXoizvs8YmZMoEap948oplYFaIP+xCnCr8l3v7znwfZwTMQPoPvqEFqUmWYqt xkJ0qaE645ihTnLqk4eq1sBLs1wPR1RJU+t6kGGAUmxqhPFxb3/1xNRPVzOGn12w S9yw+XLC6kS4PmKoxkxax4nnCx7s3e7B5e0qmYtgRTJ0GuW7Uf+T3royT0uYm0d+ ik6bmxcn00qdcHtt2HTbI+kYpken3YrF0h9Jnm9ZKT63gQSqQWL800ZVd4dAZceg FciNKs9r26fyy+L3rGCh+U9TLf6mNuWu8RstjjIGPHEPKZ9gnMgMJmikP2ghgOAd XVhs6ashXx33bZ9dIuhRx6uTNMrppsXyg6SxUyeGDYhpxsPt7uRwBswOpi6iDMZn ISSzQjrkxoNwwOfn8705fTCLhHlTZa8HS5HMK3KE7LiZv9pa1z6KTo4z+LCQSLDy FoRJhSaEsCYJsLDS5nYBoR8hE/eMvQDX1f+RZBrJDcftxx7FQ+8RtvHSJRcJK9N/ Ph/pL62NBlSbvCfn1AbisKrbbgCVLOSj/doufPvpMT2UDL0TY8UnQiyWMH1MF3tZ jJy6Si2glLwA9hu/c1NsREbA0gxMTjAREb5BjAUmlc3fuv2DWpwnkwyZNyHdm9B9 TPRoByGPvSZXa8MwY/8DUEwUQEsfDJi5jlAD4I6VFFUB72ZS7wn/mVR02fPkfOMp 3yhnGgX29OaDDiDlKw1Xwj1NybOhpZ6unDo5J3stMxlbv5TYL2Tl6egZSOSjsLmn cj5zkyUU22/93E5vfKD1CMiXx9/e4j2rRh3QCIXqaCjC9acTJ8a/k9/bp8Nz5Cir pnaCbuQsvna92nxVUqcmLlSbVIvGqlH9qm4DurhcLh59j20tX6K8AMJ90+azaYbX AJV/MCElhJg6wcN8QnCHMhiuK9+zpsUK2FQgfbcgaaNe3xGaXuoOIGQmlbAGtEkp kuauRzQ8/pwszaZuPh/5rE77z8zMut3+0E5CslB9npzNi0b0itaaRl13bBBml1xn

r6SBUw7AWapZwRx6pihvptLJaqU1IzaV5SWk0zTABR7BmR84L0+/8v/bedcPSioG

ecside21F6CcW05ywABBxDYQXM1P9qkC/2bkPkEJ0jB15P5L1+Yqb8hTlone/InR B8ktEd8+QW8o60h0seONXumTqBfAuNBkprOA3ssXLeEGB0IpeC5oGW+VSziyS9id zYq8WaehpAIf3pqwn8gsi0B/wd57T0KK91+v0Ei4z+yIdu8Kh9GTiqGvgNAeakgr ECDiXoKAwltYAn7cLKNpZaojSs2Jt+60oBA5crT04Mtgpjb9Pd/DLqWQDJTyoRVv cJRb68a0yZvVBU0yoLbox84QKLHIsA92pplS7VFrAWP65wrhs4XOf4YSF1M89Sn4 GD/yEsGVJzwGrxgCNnOZkLIKsFbI0jp21Mps5jVKoFfpPJCie3F2FB3ecS+xRpHo 5u2KOTmH0rFQ6Vu+JYCo/qWh0ERtL/8gczP7C9ehiaZfemw2bq9xrUo+6y3H9Q+Z LADwM1AkI+kzbng3R+fj4AYBvf8GTJdpBs8s/t7mZXHiXCtH6qxTMRWJx5Xuxs9F I8Ii8TA9MCEwCQYFKw4DAhoFAAQUj0/On/REYODupznP9SwYnFX92BYEFESx1MSa ho3Cv1cZYM0TzZEzlsKdAgIEAA==

quit INFO: Import PKCS12 operation completed successfully 止眠4 時就准認之司

步驟11.驗證憑證資訊。

ASA(config)#show crypto ca certificates <HeadEnd> CA Certificate Status: Available Certificate Serial Number: 01 Certificate Usage: Signature Public Key Type: RSA (1024 bits) Signature Algorithm: MD5 with RSA Encryption Issuer Name: cn=calo_root Subject Name: cn=calo_root Validity Date: start date: 13:24:35 UTC Jul 13 2017 end date: 13:24:35 UTC Jul 12 2020 Storage: config Associated Trustpoints: test HeadEnd Certificate Status: Available Certificate Serial Number: 05 Certificate Usage: General Purpose Public Key Type: RSA (2048 bits) Signature Algorithm: SHA1 with RSA Encryption Issuer Name: cn=calo_root Subject Name: hostname=Connected_2_INET-B cn=HeadEnd.david.com Validity Date: start date: 16:56:14 UTC Jul 16 2017 end date: 16:56:14 UTC Jul 16 2018 Storage: config Associated Trustpoints: HeadEnd

生成客戶端證書

步驟1.生成可匯出的RSA金鑰對。

IOS-CA(config)# crypto key generate rsa modulus 2048 label <Win7_PC> exportable
The name for the keys will be: Win7_PC
% The key modulus size is 2048 bits
% Generating 2048 bit RSA keys, keys will be exportable...
[OK] (elapsed time was 5 seconds
步驟2.配置信任點。

IOS-CA(config)# crypto pki trustpoint <Win7_PC>
IOS-CA(ca-trustpoint)#enrollment url http://10.201.180.230:80
IOS-CA(ca-trustpoint)#subject-name <cn=Win7_PC.david.com>
IOS-CA(ca-trustpoint)#revocation-check none
IOS-CA(ca-trustpoint)#rsakeypair <Win7_PC>
步驟3.對配置的信任點進行身份驗證(獲取CA證書)。

IOS-CA(config)#crypto pki authenticate <Win7_PC>
Certificate has the following attributes:
 Fingerprint MD5: DA4502F4 CEFB4F08 AAA3179B 70019185
 Fingerprint SHA1: A887F6DB 0656C7E2 857749F3 EA3D7176 8920F52F
% Do you accept this certificate? [yes/no]: yes
Trustpoint CA certificate accepted.
步驟4.註冊經過身份驗證的信任點(獲取身份證書)。

IOS-CA(config)#crypto pki enroll <Win7_PC> 8 % Start certificate enrollment .. % Create a challenge password. You will need to verbally provide this password to the CA Administrator in order to revoke your certificate. For security reasons your password will not be saved in the configuration. Please make a note of it. Password: cisco123 Re-enter password: cisco123 % The subject name in the certificate will include: cn=Win7_PC.david.com % The subject name in the certificate will include: Connected_2_INET-B % Include the router serial number in the subject name? [yes/no]: no % Include an IP address in the subject name? [no]: no Request certificate from CA? [yes/no]: yes % Certificate request sent to Certificate Authority % The 'show crypto pki certificate verbose Win7_PC' command will show the fingerprint. *Jul 17 15:21:11.343: CRYPTO_PKI: Certificate Request Fingerprint MD5: 9153E537 11C16FAE B03F7A38 775DBB92 *Jul 17 15:21:11.343: CRYPTO_PKI: Certificate Request Fingerprint SHA1: 3BC4AC98 91067707 BB6BBBFB ABD97796 F7FB3DD1 *Jul 17 15:21:15.675: %PKI-6-CERTRET: Certificate received from Certificate Authority 步驟5.驗證憑證資訊。

IOS-CA#show crypto pki certificates verbose <Win7_PC> Certificate Status: Available Version: 3 Certificate Serial Number (hex): 03 Certificate Usage: General Purpose Issuer: cn=calo_root Subject: Name: Connected_2_INET-B hostname=Connected_2_INET-B cn=Win7_PC.david.com Validity Date: start date: 13:29:51 UTC Jul 13 2017 end date: 13:29:51 UTC Jul 13 2018 Subject Key Info: Public Key Algorithm: rsaEncryption RSA Public Key: (2048 bit) Signature Algorithm: SHA1 with RSA Encryption Fingerprint MD5: 9153E537 11C16FAE B03F7A38 775DBB92

Fingerprint SHA1: 3BC4AC98 91067707 BB6BBBFB ABD97796 F7FB3DD1 X509v3 extensions: X509v3 Key Usage: A000000 Digital Signature Key Encipherment X509v3 Subject Key ID: F37266AE 61F64BD9 3E9FA80C 77455F21 5BEB870D X509v3 Authority Key ID: B5EEEEB9 31B9A06C CBD9893C 0E318810 5CA657E6 Authority Info Access: Extended Key Usage: Client Auth Server Auth Associated Trustpoints: Win7_PC Key Label: Win7_PC CA Certificate Status: Available Version: 3 Certificate Serial Number (hex): 01 Certificate Usage: Signature Issuer: cn=calo_root Subject: cn=calo_root Validity Date: start date: 13:24:35 UTC Jul 13 2017 end date: 13:24:35 UTC Jul 12 2020 Subject Key Info: Public Key Algorithm: rsaEncryption RSA Public Key: (1024 bit) Signature Algorithm: MD5 with RSA Encryption Fingerprint MD5: DA4502F4 CEFB4F08 AAA3179B 70019185 Fingerprint SHA1: A887F6DB 0656C7E2 857749F3 EA3D7176 8920F52F X509v3 extensions: X509v3 Key Usage: 8600000 Digital Signature Key Cert Sign CRL Signature X509v3 Subject Key ID: B5EEEEB9 31B9A06C CBD9893C 0E318810 5CA657E6 X509v3 Basic Constraints: CA: TRUE X509v3 Authority Key ID: B5EEEEB9 31B9A06C CBD9893C 0E318810 5CA657E6 Authority Info Access: Associated Trustpoints: test HeadEnd Win7_PC CA_Server

在Windows 7客戶端電腦上安裝身份證書

步驟1.以PKCS12格式(.p12)將命名的Win7_PC信任點匯出到FTP/TFTP伺服器(安裝在Windows 7電腦上),以在單個檔案中獲取身份證書、CA證書和私鑰。

IOS-CA(config)#crypto pki export <Win7_PC> pkcs12 <tftp://10.152.206.175/ Win7_PC.p12> password <cisco123> Address or name of remote host [10.152.206.175]? Destination filename [Win7_PC.p12]? !Writing pkcs12 file to tftp://10.152.206.175/Win7_PC.p12 ! CRYPTO_PKI: Exported PKCS12 file successfully. *Jul 17 16:29:20.310: %PKI-6-PKCS12EXPORT_SUCCESS: PKCS #12 Successfully Exported. 這是匯出檔案在客戶端電腦上的外觀。



步驟2.按Ctrl + R並鍵入mmc以開啟Microsoft管理控制檯(MMC)。

📨 Run	
	Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.
<u>O</u> pen:	mmc 🗸
	This task will be created with administrative privileges.
	OK Cancel <u>B</u> rowse

步驟3.選擇OK。

Gonsole1 - [Console Root]			
File Action View Favorites Wind	low Help		_ = = ×
Console Root	Name		Actions
		There are no items to show in this view	Console Root
			More Actions

步驟4.導航到**檔案>新增/刪除管理單元**。

Gonsole1 - [Console Root]		
File Action View Favorites Wind	ow Help	_ & ×
Console Root	Add or Remove Snap-ins	Actions
	You can select snap-ins for this console from those available on your computer and configure the selected set of snap-ins. For extensible snap-ins, you can configure which extensions are enabled.	Console Root
	Available snap-ins: Selected snap-ins:	More Actions
	Snap-in Vendor Console Root Edit Extensions	
	ActiveX Control Microsoft Cor Remove Remove	
	Certificates Microsoft Cor	
	Component Services Microsoft Cor	
	Device Manager Microsoft Cor Add >	
	Disk Management Microsoft and	
	Folder Microsoft Cor	
	Group Policy Object Microsoft Cor	
	P Security Monitor Microsoft Cor Picrosoft Cor	
	Link to Web Address Microsoft Cor 🛫	
	Description: The ActiveX Control snap-in enables you to add an MMC node with a results view containing an ActiveX control.	
	OK Cancel	

步驟5.選擇Certificates > Add > Computer Account。

Console1 - [Console Root]		
File Action View Favorites Window Help		_ 8 ×
Console Root Name		Actions
		Console Root
Add or Remove Snap-ins	23	More Actions
You can select snap-ins for this console from those available on your computer and configure the selected s extensible snap-ins, you can configure which extensions are enabled.	e Certificates snap-in	
Available span-ins: Selected span-ins:		
Spap.in Vender A	This snap-in will always manage certificates for:	
Active Y Control Microsoft Cor	My user account	
Z Authorization Manager Microsoft Cor	Service account	
Certificates Microsoft Cor	Computer account	
Component Services Microsoft Cor	0	
Ecomputer Managem Microsoft Cor		
Disk Management Microsoft and		
Event Viewer Microsoft Cor		
Folder Microsoft Cor		
Group Policy Object Microsoft Cor		
TD Security Monitor Microsoft Cor		
(a) Link to Wab Addrees Microsoft Cor.		
Description:		
The Certificates snap-in allows you to browse the contents of the certificate stores for yourself, a service.		
,,	< Back	Next > Cancel
		Carloor
	OK Cancel	

步驟6.選擇下**一步**,

Console Root Actions Add or Remove Snap-ins Console Root You can select snap-ins for this console from those available on your computer and configure the select extensible snap-ins, you can configure which extensions are enabled. Select display Available snap-ins: Selected snap-ins: Selected snap-ins: Select display ActiveX Control Microsoft Cor Extensible snap-ins: Select display Select display ActiveX Control Microsoft Cor Active Console Root His snap-in will always manage: Description (always manage) This snap-in will always manage: Description (always manage) Description (always manag	Console⊥-[Console Koot] File Action View Favorites Window Help ⇔ 🕡 📴 🔽 🗊	
Description: The Certificates snap-in allows you to browse the contents of the certificate stores for yourself, a server the certificate store stor	Console Root Name Add or Remove Snap-ins You can select anap-ins for this console from those available on your computer and configure the select extensible snap-ins; you can configure which extensions are enabled. Available snap-ins: Selected snap-ins: Snap-in Vendor ActiveX Control Microsoft Cor Authorization Manager Microsoft Cor Component Services Microsoft Cor Component Services Microsoft Cor Disk Management Microsoft Cor Folder Microsoft Cor P Security Policy Monitor Microsoft Cor Folder	ns I

步驟7.**完成**。

🚡 Console1 - [Console Root]						
File Action View Favorites Win	dow Help					- 8 ×
Conrola Poet	1					
Console Root	Name				Actions	
	Add or Remove Snap-ins			×	Console Root	^
	You can select snap-ins for t extensible snap-ins, you can Available snap-ins:	his console from those availa configure which extensions	ble on your computer and configure the selected s are enabled. Selected snap-ins:	et of snap-ins. For	More Actions	•
	Snap-in	Vendor ^	Console Root	Edit Extensions		
	ActiveX Control	Microsoft Cor	Certificates (Local Computer)	Remove		
	Authorization Manager	Microsoft Cor		- Techore		
	Certificates	Microsoft Cor E		Movello		
	Computer Managem	Microsoft Cor				
	Device Manager	Microsoft Cor	dd S	Move Down		
	Disk Management	Microsoft and				
	8 Event Viewer	Microsoft Cor				
	Folder	Microsoft Cor				
	Group Policy Object	Microsoft Cor				
	IP Security Policy M	Microsoft Cor				
	Link to Web Address	Microsoft Cor		Advanced		
	A					
	Description:					
	The Certificates snap-in allo	ws you to browse the conter	nts of the certificate stores for yourself, a service,	or a computer.		
				OK Cancel		
	L _{1.}					

步驟8.選擇**OK**。

步驟9.轉到Certificates(Local Computer)>Personal>Certificates,按一下右鍵資料夾並導航到All Tasks>Import:

Console1 - [Console Root\Certificates (Loo	cal Computer)\Pers	onal\Certificates]						- • •
🖀 File Action View Favorites Wind	ow Help							- 8 ×
🗢 🄿 🙋 📰 📋 🙆 📑								
Console Root	Issued To	^	Issued By	Expiration Date	Intended Purposes	Friendly Na	Actions	
 Certificates (Local Computer) Personal 	🛱 DRIVERAP-6KU	JZH	DRIVERAP-6KUZH	7/13/2022	<all></all>	<none></none>	Certificates	^
Certificates	•	Request New	Certificate				More Actions	•
Enterprise View		Import						
 Intermedia Trusted Pu New Window from 	om Here	Advanced Op	erations +					
Contrusted (New Taskpad Vie	ew							
Trusted Per Refresh								
Other Peop Export List Ams								
CanaryCert Help								
McAfee Trust								
PolicyCertStore PolicyCertStore PolicyCertStore								
Certificate Enrollment Requests								
SMS								
SPC Trusted Devices								
Add a certificate to a store	•		III			4	1	

Certificate Import Wizard



Welcome to the Certificate Import Wizard

This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store.

A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.

To continue, click Next.

	< De els	Nexts	Canaal
	< back	Next >	Cancel

步驟10.按一下「Next」。指示儲存PKCS12檔案的路徑。

Certificate Import Wizard	×		
File to Import			
Specify the file you want to import.			
File name:			
C:\TFTP-Root\Win7_PC.p12 Browse			
Note: More than one certificate can be stored in a single file in the following formats:			
Personal Information Exchange- PKCS #12 (.PFX,.P12)			
Cryptographic Message Syntax Standard-PKCS #7 Certificates (.P7B)			
Microsoft Serialized Certificate Store (.SST)			
Learn more about <u>certificate file formats</u>			
< Back Next > Canc	el		

步驟11.再次選擇**下一步**,並鍵入在*crypto pki export <Win7_PC> pkcs12 <tftp://10.152.206.175/ Win7_PC.p12> password <cisco123>命令中輸入的密*碼

Certificate Import Wizard
Password To maintain security, the private key was protected with a password.
Type the password for the private key.
Password:
Enable strong private key protection. You will be prompted every time the private key is used by an application if you enable this option.
Mark this key as exportable. This will allow you to back up or transport your keys at a later time.
☑ Include all extended properties.
Learn more about protecting private keys
< Back Next > Cancel

步驟12.選擇下**一步**。

Certificate Import Wizard	×
Certificate Store Certificate stores are system areas where certificates are kept.	
Windows can automatically select a certificate store, or you can specify a location for the certificate.	
Place all certificates in the following store Certificate store:	
Personal Browse	
Learn more about <u>certificate stores</u>	
< Back Next > Cancel	

步驟13.再次選擇Next。



步驟14.選擇**完成**。

Certificate Import Wizard
The import was successful.
ОК

步驟15.選擇OK。現在您將看到已安裝的證書(CA證書和身份證書)。

Console1 - [Console Root\Certificates (Lo	cal Computer)\Personal\Certificates]						
File Action View Eavorites Wind	ow Help						
Console Root	Issued To	Issued By	Expiration Date	Intended Purposes	Friendly Na	Actions	
A Personal	alo_root	calo_root	7/12/2020	<all></all>	cn=calo_ro	Certificates	^
Certificates	C DRIVERAP-6KUZH	DRIVERAP-6KUZH	7/13/2022	<all></all>	<none></none>	More Actions	•
Trusted Root Certification Author	Win/_PC.david.com	calo_root	//13/2018	Server Authenticati	cn=Win/_P		
Enterprise Trust							
Intermediate Certification Author							
Trusted Publishers							
Dirtusted Certificates Third-Party Root Certification Aut							
Trusted People							
Other People							
Ams							
CanaryCertStore							
InjectorCertStore							
McAfee Trust							
Policyceristore Remote Desktop							
Certificate Enrollment Requests							
Smart Card Trusted Roots							
SMS							
▷ 🚞 SPC							
Trusted Devices							
	•	III			+		
Personal store contains 3 certificates.							

步驟16.將CA證書從**證書(本地電腦)>個人>證書**拖放到**證書(本地電腦)>受信任的根證書頒發機 構>證書。**

a Console1 - [Console Root\Certificates (Local Computer)\Trusted Root Certification Authorities\Certificates]							- • ×
🚡 File Action View Favorites Wind	ow Help						- 8 ×
Console Root	Issued To	Issued By	Expiration Date	Intended Purposes	Friendly ^	Actions	
Certificates (Local Computer)	AddTrust External CA Root	AddTrust External CA Root	5/30/2020	Server Authenticati	The USE	Certificates	
A Personal	Baltimore CyberTrust Root	Baltimore CyberTrust Root	5/12/2025	Server Authenticati	DigiCert	More Actions	•
Certificates	🙀 calo_root	calo_root	7/12/2020	<all></all>	cn=calo		
Cartificates	Certum CA	Certum CA	6/11/2027	Server Authenticati	Certum	calo_root	^
Enterprise Trust	Certum Trusted Network CA	Certum Trusted Network CA	12/31/2029	Server Authenticati	Certum E	More Actions	•
Intermediate Certification Author	🔄 Cisco Root CA 2048	Cisco Root CA 2048	5/14/2029	<all></all>	<none></none>		
Trusted Publishers	🔄 Cisco Root CA M1	Cisco Root CA M1	11/18/2033	<all></all>	<none></none>		
Untrusted Certificates	🔄 Cisco Root CA M1	Cisco Root CA M1	11/18/2033	<all></all>	<none></none>		
Third-Party Root Certification Aut	🔄 Cisco Root CA M2	Cisco Root CA M2	11/12/2037	<all></all>	<none></none>		
Trusted People	🔄 Cisco RXC-R2	Cisco RXC-R2	7/9/2034	<all></all>	<none></none>		
Other People	Class 3 Public Primary Certificat	Class 3 Public Primary Certificatio	8/1/2028	Secure Email, Client	VeriSign		
Ams	COMODO RSA Certification Au	COMODO RSA Certification Auth	1/18/2038	Server Authenticati	COMOE		
CanaryCertStore	Copyright (c) 1997 Microsoft C	Copyright (c) 1997 Microsoft Corp.	12/30/1999	Time Stamping	Microso		
InjectorCertStore	Deutsche Telekom Root CA 2	Deutsche Telekom Root CA 2	7/9/2019	Secure Email, Serve	Deutsch		
McAfee Trust	🔄 DigiCert Assured ID Root CA	DigiCert Assured ID Root CA	11/9/2031	Server Authenticati	DigiCert		
PolicyCertStore	🔄 DigiCert Global Root CA	DigiCert Global Root CA	11/9/2031	Server Authenticati	DigiCert		
Remote Desktop	DigiCert High Assurance EV Ro	DigiCert High Assurance EV Root	11/9/2031	Server Authenticati	DigiCert		
Certificate Enrollment Requests	🛱 DRIVERAP-6KUZH	DRIVERAP-6KUZH	7/13/2022	<all></all>	<none></none>		
Smart Card Trusted Roots	🛱 DRIVERAP-6KUZH.cisco.com	DRIVERAP-6KUZH.cisco.com	1/12/2021	<all></all>	<none></none>		
	DST Root CA X3	DST Root CA X3	9/30/2021	<all></all>	<none></none>		
Trusted Devices	DST Root CA X3	DST Root CA X3	9/30/2021	<all></all>	<none></none>		
	Entrust Root Certification Auth	Entrust Root Certification Authority	11/27/2026	Server Authenticati	Entrust		
	Entrust Root Certification Auth	Entrust Root Certification Authori	12/7/2030	Server Authenticati	Entrust.		
	Entrust.net Certification Author	Entrust.net Certification Authority	7/24/2029	Server Authenticati	Entrust		
۰	Enuifay Secure Certificate Auth	Equifav Secure Certificate Authority	8/22/2018	Servire Emsil Serve	GeoTrue *		
Trusted Root Certification Authorities store co	ntains 60 certificates.						

Console1 - [Console Root/Certificates (Local Computer)\Personal\Certificates]							
	ow help						X
 File Action View Favorites Windd File Action View Favorites Windd Console Root Certificates (Local Computer) Personal Certificates Certificates Certificates Certificates Certificates Certificates Certificates Trusted Root Certification Author Trusted People Mans Coher People Ams CanaryCertStore McAfee Trust PolicyCertStore 	w Help Issued To Call DRIVERAP-6KUZH	Issued By DRIVERAP-6KUZH calo_root	Expiration Date 7/13/2022 7/13/2018	Intended Purposes <all> Server Authenticati</all>	Friendly Na <none> cn=Win7_P</none>	Actions Certificates More Actions	X
Remote Desktop Certificate Enrollment Requests Smart Card Trusted Roots SMS SPC Trusted Devices	۲	III			Þ		
Personal store contains 2 certificates.							

如何在Android流動裝置上安裝身份證書

附註:Android支援副檔名為.pfx或.p12的PKCS#12金鑰儲存檔案。

附註:Android僅支援DER編碼的X.509 SSL證書。

步驟1。從PKCS12(.p12)格式的IOS CA伺服器匯出使用者端憑證後,透過電子郵件將檔案傳送到 Android裝置。安裝完畢後,請點選檔案的名稱以啟動自動安裝。(**不下載檔案**)

🗆 🖬 ±	7.	al 53%	6 8 7:24	PM
÷			\simeq	:
				r.
Android S	martnhone n12	+	۸	
Permona_0	n non ignition re. p/12	-	1.00	
*			*	
Reply	Reply all		Forward	

步驟2.輸入用於匯出證書的密碼,在本例中,密碼為cisco123。

Extract certificate
Enter the password to extract the certificates.
CANCEL OK

步驟3.選擇OK並輸入Certificate name。它可以是任何單詞,在本示例中,名稱為Android ID Cert。



步驟4.選擇「OK」,系統將顯示消息「Android ID Cert installed」。

步驟5。若要安裝CA憑證,請以base64格式從IOS CA伺服器擷取該憑證,並以.crt擴充檔儲存該憑 證。通過電子郵件將檔案傳送到Android裝置。這一次,您需要透過貼上檔案名稱旁邊的箭頭來下載 檔案。

⊟ ±		7 🛋 51	6:54	PI
-			\simeq	:
calo_ro	oot.crt	<u>+</u>	۵	
*	~		*	
Deplu	Reply all		Forward	

6:54 PM Tue, July 18	۰ 🗢
🗟 🛇 🔹	⊗ 🛞
Wi-Fi Location Sound	Auto Bluetooth rotate
*•	Outdoors
calo_root.crt Download complete.	6:54 PM
NOTIFICATION SETTINGS	CLEAR
and the second s	
the second se	
Calo_root.crt	± 🛆
Reply Reply all	Forward
Emergency calls	only

步驟6.導覽至Settings和Lock screen and security。



步驟7.選擇Other security settings。

7 🛋 50% 🛢 6:57 PM

Lock screen and security

Notifications on lock screen

Show content

Secure lock settings

Set your secure lock functions, such as Auto lock and Lock instantly with Power key.

Security

Find My Mobile

Locate and control your device remotely using your Samsung account.

Unknown sources

Allow installation of apps from sources other than the Play Store.

Encrypt device

Protect your device by encrypting its data.

Encrypt SD card

No SD card inserted

Other security settings

Change other security settings, such as those for security updates and credential storage.

步驟8.導航至**從裝置儲存安裝。**

🖬 🛓

A 🖂 🖬 🛓

3 📶 54% 🛢 7:29 PM

Other security settings

View security certificates

Display trusted CA certificates.

User certificates

View user certificates.

Install from device storage

Install certificates from storage.

Clear credentials

Remove all certificates.

Advanced

Trust agents

Perform selected actions when trusted devices are connected.

Pin windows

Off

Usage data access

View which applications can access your device's usage history.

步驟9.選擇.crt檔案並點選完成。



步驟10.輸入憑證名稱。它可以是任何單詞,在本例中,名稱為calo_root-1。



步驟10.選擇OK,您將看到消息「calo_root-1 installed」。

Select file	
C calo_root-1.crt	
calo_root-1 installed.	

步驟11.若要驗證是否已安裝身份證書,請導航到Settings/Lock Screen and Security/Other > Security Settings/User Certificates/System**頁籖。**

A = ± ± = ±

🖀 📶 54% 🖹 7:45 PN

Other security settings

Storage type

Back up to hardware.

View security certificates

Display trusted CA certificates.

User certificates

View user certificates.

Install from device storage

Install certificates from storage.

Clear credentials

Remove all certificates.

Advanced

Trust agents

Perform selected actions when trusted devices are connected.

Pin windows

JII

Lloono data annon



Android_Smartphone.david.com

步驟12.要驗證CA證書是否已安裝,請導航到Settings/Lock螢幕和security/Other security settings/View security certificates/User頁籤。

A = ± ± = ±

🖀 📶 54% 🖹 7:45 PN

Other security settings

Storage type

Back up to hardware.

View security certificates

Display trusted CA certificates.

User certificates

View user certificates.

Install from device storage

Install certificates from storage.

Clear credentials

Remove all certificates.

Advanced

Trust agents

Perform selected actions when trusted devices are connected.

Pin windows

JII

Lloono data annon

A 🖬 ± ± 🖬 ±	常 ⊿l 54% ≣ 7:45 PM					
← View security certificates						
SYSTEM	USER					
calo_root						

為使用IKEv2的RA VPN配置ASA頭端

步驟1。在ASDM上,導航到Configuration>Remote Access VPN > Network(client)Access> Anyconnect Connection Profiles。在面向VPN客戶端的介面上選中IPSec(IKEv2)access, Allow Access框(Enable Client Services選項不是必需的)。

步驟2.選擇Device Certificate,然後從Use same device certificate for SSL and IPSec IKEv2中刪除 檢查標籤。

步驟3.為IPSec連線選擇頭端證書,為SSL連線選擇 — 無。

此選項將實施加密ikev2、加密ipsec、加密動態對映和加密對映配置。

Cisco ASDM 7.8(1)150 for ASA - 192.168.0.254								- 🗗 🔀
File View Tools Wizards Window Help							Type topic to search Go	abab
Home Configuration 😥 Monitoring 🔲 Sa	ave 💽 Refresh 🤇	Back O Forw	ard 🢡 Help					cisco
Remote Access VPN	Configuration > R	emote Access V	PN > Network (Client) Access > AnyConnect	Connection Profiles			
Introduction Method: (Clent) Access Method: (Clent) Access Method: (Clent) Access Anconcet Customization (Acaization Anconcet Customization (Acaization Anconcet Clent Profile Anconcet Clent Profile Anconcet Clent Software	The security applia IPsec (IKEv2) tunn Access Interfaces — Enable Cisco A SSI access must b	nce automatically o el as well as SSL tu nyConnect VPN Clin	deploys the Cisco AnyCo nnel with Datagram Tra ent access on the interfa	nnect VPN Client to remote nsport Layer Security (DTLS) aces selected in the table be	users upon connection. Th tunneling options. low	e initial client deployment requires end-user adminis	rative rights. The Cisco AnyConnect VPN Cli	ent supports
Group Policies	SSC access must be	SCI Access	on Anyconnect clent to	IReac (IVEv2) Acces	(web cauloi) .			
 IPsec(IKEv1) Connection Profiles IPsec(IKEv2) Connection Profiles 	Interface	All Access	Earth OT C	IPBEC (INEV2) ACCES	,	Device Certificate		
Secure Mobility Solution	outside	Allow Access	Enable DTLS	Allow Access	Enable Client Services			
Address Assignment Advanced	inside					Port Settings		
Clientless SSL VPN Access								
B Cetificate Management B Cetificate Management B Cetificate Management B Cetificate Management D Cetificate Management	Login Page Setting – Allow user to s Shutdown port Connection Profiles Connection profile Add Z Edi	elect connection pr al login page. (tunnel group) spr (tunnel group) spr	rofile on the login page. ecifies how user is authe	Inticated and other parameter Go Image Match Case	ers. You can configure the	mapping from certificate to connection profile <u>here</u> .		
	Name	501	Enabled	TRees Enabled	Aliaco	ac Authentication Mathod	Group Policy	
	DefaultRAGroup	000		a occ a nanca	7	AAA(LOCAL)	DfltGrpPolicy	
	DefaultWEBVPNG	oup			7	AAA(LOCAL)	DfltGrpPolicy	
						Specify Device Certificate		
Device Setup Device Setup Frewal Great Ste-to-Site VPN Device Management	Let group URL	take precedence if	group URL and certifica	ite map match different conr	ection profiles. Otherwise	Device certificate is a digital certificate that ident Use the same device certificate for SSL and I Device Certificate for SSL Connection:	fles this ASA to the clients. Pisec IXEV2 : ddhostname=Connected_2_INET=8, on=He Manage Certificates	▼ dĒnd.da ▼

這是組態在指令行介面(CLI)上的樣子。

crypto ikev2 policy 1 encryption aes-256 integrity sha group 5 prf sha lifetime seconds 86400 crypto ikev2 enable outside

crypto ikev2 remote-access trustpoint HeadEnd crypto ipsec ikev2 ipsec-proposal AES256 protocol esp encryption aes-256 protocol esp integrity sha-1 md5

crypto dynamic-map Anyconnect 65535 set ikev2 ipsec-proposal AES256 crypto map outside_map 65535 ipsec-isakmp dynamic Anyconnect crypto map outside_map interface outside

步驟4.導航到Configuration > Remote Access VPN > Network(Client)Access > Group Policies以建 立組策略

Fautra in ar		- / / 1	
Add Internal Group Policy			
General	Name: GP_David		
⊕ Advanced	Banner: 👽 Inherit		
	SCEP forwarding LIBL : I Inherit		
			Colum
	Address Pools: V Inhent		Select
	IPv6 Address Pools: V Inherit		Select
	More Options		\$
	Tunneling Protocols:	inherit Clientiess SSL VPN SSL VPN Client IPsec IKEv1 V IPsec IKEv2 LZTP/IPsec	
	Filter:	☑ Inherit	Manage
	Access Hours:	✓ Inherit	Manage
	Simultaneous Logins:	✓ Inherit	
	Restrict access to VLAN:	🖉 Inherit 🗸 🗸	
	Connection Profile (Tunnel Group) Lock:	✓ Inherit	
	Maximum Connect Time:	Inherit Unlimited minutes	
	Idle Timeout:	Inherit None minutes	
	Security Group Tag (SCT):		
	Security group ray (501).		
	On smart card removal:		
	Periodic Certificate Authentication Interva	I: V Inherit Unimited hours	
Find:	Next Previou	S	
		OK Cancel Help	

在CLI上。

group-policy GP_David internal
group-policy GP_David attributes
vpn-tunnel-protocol ikev2

步驟5.導航到Configuration > Remote Access VPN > Network(Client)Access > Address Pools,然 後選擇Add以建立IPv4池。

Cisco ASDM 7.8(1)150 for ASA - 192.168.0.254				
File View Tools Wizards Window Help			Type topic to search Go	ababa
Home 🖓 Configuration 🔯 Monitoring 🎧 Save	e 🔇 Refresh 🔇 Back 🔘 Forward 🤶 Help			cisco
Remote Access VPN 🗗 🖗	Configuration > Remote Access VPN > Network (Client) Access	> Address Assignment > Address Pools		
Remote Access VPI Remote Access VPI	Configuration > Remote Access VFN > Network (Clent) Access Configure named IP Address Pools. The IP Address Pools car clustering.	> Address Assignment > Address Pool: to be used in either a VPN [Pase(I)SU1) Connection Profiles, Am/Connect Connec so Ending Address,Number of Addresses [192, 166, 50, 100 Edit IPv4 Pool Name: ACPool Starting IP Address: [192, 166, 50, 1] Ending IP Address: [192, 166, 50, 1] Subnet Mask: 255, 255, 255, 0 CK Cancel Help	ction Profiles, Group Policies configuration , or in <u>interfaces</u> configuration Subnet Mask/Prefix Length 255/255/255/0	related to ASA
Device Management				
»		Apply Reset		

ip local pool ACPool 192.168.50.1-192.168.50.100 mask 255.255.255.0

步驟6.導航到Configuration > Remote Access VPN > Network(Client)Access > IPSec(IKEv2)Connection Profiles,然後選擇Add以建立新的隧道組。





```
tunnel-group David type remote-access
tunnel-group David general-attributes
address-pool ACPool
default-group-policy GP_David
authentication-server-group LOCAL
tunnel-group David webvpn-attributes
authentication certificate
tunnel-group David ipsec-attributes
ikev2 remote-authentication certificate
ikev2 local-authentication certificate HeadEnd
```

步驟7.導航到Configuration > Remote Access VPN > Network(Client)Access > Advanced > IPsec > Certificate to Connection Profile maps > Policy, 然後選中Used the configured rules to math a certificate to a Connection Profile框。





tunnel-group-map enable rules

步驟8.導航到Configuration > Remote Access VPN > Network(Client)Access > Advanced > IPsec > Certificate to Connection Profile maps > Rules,然後建立新的證書對映。選擇Add並將其關聯到隧 道組。在本示例中,隧道組名為David。

Cisco ASDM 7.8(1)150 for ASA - 192.168.0.254						S
File View Tools Wizards Window Help				Type topic to search	Go	abab
Home 🖓 Configuration 🔯 Monitoring 🔚 Sa	ave 💽 Refresh 🚺 Back 🔘 Forv	rard 🦻 Help				CISCO
Remote Access VPN	Configuration > Remote Access V	PN > Network (Client) Access > Advanced > IPsec > 0	Certificate to Connection Profile Maps > Rule	<u>5</u>		
Introduction AnyConnect Connection Profiles AnyConnect Construction Profiles AnyConnect Class Polices AnyConnect Class Polices AnyConnect Class Polices Presc(IKE*1) Connection Profiles Presc(IKE*1) Co	Define rules to map certificates to de Certificate to Connection Profile Maps Add Edt Deletel Fin Map Name Mapping Criteria	d: O Connect or clentless SSL connection profiles (tunnel) d: O C Match Case Rule Priority	proups). Use the bottom table to configure certificat Mapped to Connection Profi	e fields together with their matching oriteria for t	he selected	rule.
Address Pools Address Pools Address Pools Advanced AnyConnet Cluston Attributes AnyConnet Cluston Attributes AnyConnet Cluston Attributes AnyConnet Cluston Attributes Pools Po	Add Eds Add Centif Field Configure a Configure a	cate Matching Rule certificate matching rule and associate it with a connection pro- tating rule and assigns a priority to the rule with lower value be ignored. © Existing DefaultCertifi @ New CERT_MAP 10 Connection Profile: David V 0 OK Cancel	If it. The rule priority uniquely identifies the shwing greater priority. Rules that are not ateMap	Value		
Ste-to-Site VPN			Apply Reset			

在CLI上。

欄位:發行商

操作員:包含

值:calo_root

在CLI上。

crypto ca certificate map CERT_MAP 10

issuer-name co calo_root

步驟10.使用要使用的IP池網路建立對象,以便在Configuration > Firewall > Objects > Network Objects/Groups> Add**處新增(網路地址轉換)**NAT**免除規**則。

Cisco A M 7.8(1)150 for ASA - 192.168.0.254							D	
File View Tools Wizards Window Help						Type topic to search Go	alulu	
Home 🍪 Configuration 🔯 Monitoring 🌄 Sav	ve 🔇 Refresh 🔇 Back 🔘 Forwa	rd 🧖 Help					CISCO	
Firewall 🗇 🖗	Configuration > Firewall > Objects	> <u>Network Objects/Grou</u>	IDS					
2 Access Rules	🗣 Add 👻 🗹 Edit 📋 Delete 🔍 W	here Used 🔍 Not Used						
Service Policy Rules	Filter:							
AAA Rules	Name	TP Address		Netmack	Description	Object NAT Address		
Public Servers	Network Objects	1 100 000		The Grinday	besaptori	objection Address		
URL Filtering Servers	anv							
	- 🏟 anv4							
2 Identity Options	- <a> any6							
-Za Identity by TrustSec	- A inside-network	10.88.243.0		255.255.255.128				
Network Objects /Groups	NETWORK OBJ 192.168.50.	192.158.50.0		255.255.255.0				
Service Objects/Groups	outside-network	192.168.0.0		255.255.255.0				
- 😴 Local Users	- 3 224.0.0.251	224.0.0.251						
Local User Groups		224.0.0.252						
		Edit Network Name: Type: IP Version: IP Address: Netmask: Description:	rk Object NETWORK_OBJ Network @ IPv4	J_192.168.50.0_24 ₽v6	•			
		NAT			*			
Device Setup			OK	Cancel H	ielp			
Firewall								
Remote Access VPN								
Site-to-Site VPN								
Device Management				Apply	Reset			

在CLI上。

object network NETWORK_OBJ_192.168.50.0_24 subnet 192.168.50.0 255.255.255.0

步驟11.導航到**Configuration > Firewall > NAT Rules**,然後選擇**Add**為RA VPN流量建立NAT免除規 則。

Cisco ASDM 7.8(1)150 for ASA - 192.168.0.254								
File View Tools Wizards Window Help							Type topic to search Go	alate
📸 Home 🦓 Configuration 🔯 Monitoring 🔚 Sav	re 💽 Refresh 🚺 B	ack 😱 Forward 🦻 Help						cisco
Firewall 0 P	Configuration > Firev	vall > NAT Rules					Addresses Services	
Access Rules	🗣 Add 👻 🗹 Edit 👔	🕞 Edit NAT Rule					Addresses	ΞΦ×
Q. Service Policy Rules	Match Criteri						💠 Add 👻 📝 Edit 🏢 Delete 🔍 Where	Used Q Not Used
AAA Rules	#	Match Criteria: Original Packet —	,	7		Options	Filter:	Filter Clear
Filter Rules	Source Intr	Source Interface:	inside	Destination Interface:	outside 👻	No Drawn	Name	
URL Filtering Servers	"Network Object" N	Source Address:	any	Destination Address:	<_OBJ_192.168.50.0_24	NOPTOXY	-Network Objects	
Threat Detection				Service:	any –		🦚 any	
Jentity Options								
E- Colects		Action: Translated Packet	(m	٦			- I any6	
Network Objects/Groups		Source NAT Type:	Static				Inside-network/25 Inside-network/25 Inside-network/25	4
Local Users		Source Address:	Original	Destination Address:	Original		outside-network/24	
Local User Groups		Use one-to-one address transl	ation					
Security Group Object Groups		PAT Pool Translated Address:		Service:	Original			
Inspect Maps		Decend Dabia		1 - CONTROL				
Regular Expressions								
Time Ranges		Extend PAT uniqueness to p	er destination instead of per	interface				
Communications		Translate TCP and UDP ports	s into flat range 1024-65535	Include range 1-102	13			
I → U Advanced		Fall through to interface PAT						
		Use IPv6 for source interface P	PAT	Use IPv6 for dest	ination interface PAT			
		Options						
		T Enable rule						
		Translate DNS replies that mat	ch this rule					
		Disable Proxy ARP on egress in	nterface					
		Lookup route table to locate eg	gress interface					
S. Device Setup		Direction: Both -						
		Description:						
Star Firewall								
Remote Access VPN			OK Cancel	Help				
Site-to-Site VPN								
Device Mapagement	•		m) F		
20 *			Apply	eset				

在CLI上。

nat (inside,outside) source static any any destination static NETWORK_OBJ_192.168.50.0_24 NETWORK_OBJ_192.168.50.0_24 no-proxy-arp route-lookup

這是用於此示例的完整ASA配置。

```
interface GigabitEthernet1/1
nameif outside
security-level 0
ip address 10.88.243.108 255.255.255.128
object network NETWORK_OBJ_192.168.50.0_24
subnet 192.168.50.0 255.255.255.0
nat (inside,outside) source static any any destination static NETWORK_OBJ_192.168.50.0_24
NETWORK_OBJ_192.168.50.0_24
ip local pool ACPool 192.168.50.1-192.168.50.100 mask 255.255.255.0
crypto ikev2 policy 1
encryption aes-256
integrity sha
group 5
prf sha
lifetime seconds 86400
crypto ikev2 enable outside
crypto ikev2 remote-access trustpoint HeadEnd
group-policy GP_David internal
group-policy GP_David attributes
vpn-tunnel-protocol ikev2
tunnel-group David type remote-access
tunnel-group David general-attributes
address-pool ACPool
default-group-policy GP_David
authentication-server-group LOCAL
tunnel-group David webvpn-attributes
authentication certificate
tunnel-group David ipsec-attributes
ikev2 remote-authentication certificate
ikev2 local-authentication certificate HeadEnd
tunnel-group-map enable rules
crypto ca certificate map CERT_MAP 10
issuer-name co calo_root
tunnel-group-map CERT_MAP 10 David
crypto ipsec ikev2 ipsec-proposal AES256
protocol esp encryption aes-256
protocol esp integrity sha-1 md5
crypto dynamic-map Anyconnect 65535 set ikev2 ipsec-proposal AES256
crypto map outside map 65535 ipsec-isakmp dynamic Anyconnect
crypto map outside_map interface outside
配置Windows 7內建客戶端
```

步驟1.導覽至控制面板>網路和Internet >網路和共用中心。

Control Panel	Network and Internet Network and Sharing Center	 ✓ ✓	م
Control Panel Home	View your basic network information and set up connection	ns	• 9
Manage wireless networks	📃 🦳 🧊 ————	See full map	
Change adapter settings	DRIVERAP-6KUZH cisco.com	Internet	
Change advanced sharing settings	(This computer) View your active networks	Connect or disconnect	
	cisco.com Access type: Domain network Connections:	Internet Wireless Network Connection (blizzard)	E
	Change your networking settings		
	📷 Set up a new connection or network		
	Set up a wireless, broadband, dial-up, ad hoc, or VPN connection; o	or set up a router or access point.	
See also	Connect to a network		
HomeGroup	Connect or reconnect to a wireless, wired, dial-up, or VPN network	connection.	
Internet Options	Choose homegroup and sharing options		
windows FireWall	Access files and printers located on other network computers, or ch	aange sharing settings.	-

步驟2.選擇**設定新的連線或網路**。

🚱 🚽 Set Up a Connection or Network	
Choose a connection option	
 Connect to the Internet Set up a wireless, broadband, or dial-up connection to the Internet. Set up a new network Configure a new router or access point. Manually connect to a wireless network Connect to a hidden network or create a new wireless profile. Connect to a workplace Set up a dial-up or VPN connection to your workplace. Set up a dial-up connection Connect to the Internet using a dial-up connection. 	
	Next Cancel

步驟3.選擇**連線到工作區**和下一步。



步驟4.選擇否,建立新連線和下一步。



步驟5.選擇**Use my Internet connection(VPN)**,然後在Internet address欄位上新增HeadEnd certificate Common Name(CN**)字元**串。在**Destination Name**欄位中,鍵入連線的名稱。它可以是 任何字串。請確保選中**Don't connect now;只需設定它,我可以在以後連線**機箱。

Connect to a Workplace	e							
Type the Internet add	lress to connect to							
Your network administrato	Your network administrator can give you this address.							
Internet address:	HeadEnd.david.com							
Destination name:	RA VPN to ASA with IKEv2							
Use a smart card								
Allow other people This option allows a	to use this connection anyone with access to this computer to use this connection.							
Don't connect now,	just set it up so I can connect later							
	Ne	xt Cancel						

步驟6.選擇下**一步**。

🚱 🗽 Connect to a Workpla	ce	
Type your user nam	e and password	
User name:	1]
Password:]
	Show characters Remember this password	
Domain (optional):]
		Create Cancel

步驟7.選擇Create。



步驟8.選擇**關閉**並導航到**控制面板>網路和Internet >網路連線**。選擇已建立的網路連線並按一下右 鍵它。選擇**屬性**。

RA VPN to ASA wi	th IKEv2			VirtualBox Host		
WAN Miniport (IK	Ev2	Connect				
VMware Network	Ad	Status				
VMware Virtual Etl	her	Set as Default Connection				
		Create Co	ру			
		Create Sh	ortcut			
	۲	Delete				
	۲	Rename				
	۲	Propertie	s			

步驟9.在**General**索引標籤中,您可以驗證頭端的適當主機名是否正確。您的電腦會將此名稱解析為 用於連線RA VPN使用者的ASA IP地址。

📱 RA VPN	to ASA	with IKEv.	2 Properties			×	
General	Options	Security	Networking	Sharing			
Host nar 157.54.0	me or IP a 0.1 or 3ffe:	ddress of c :1234::111	lestination (su 1):	ch as micro	osoft.com o	r	
HeadEr	nd.david.c	om					
- First co	onnect						
Wind	lows can f net, before	irst connectivity inst connection in the connection of the connect	ct to a public n stablish this vi	ietwork, su irtual conne	uch as the ection.		
	Dial another connection first:						
See our online <u>privacy statement</u> for data collection and use information.							
				ОК	Cano	el	

步驟10.導航到Security頁籤,然後選擇IKEv2作為VPN的型別。在Authentication部分中選擇Use machine certificates。

RA VPN to ASA with IKEv2	Properties
General Options Security	Networking Sharing
Type of VPN:	
IKEv2	•
Data encryption:	Advanced settings
Require encryption (disconne	ect if server declines) 🔹
Authentication	
O Use Extensible Authention	ation Protocol (EAP)
	· · ·
·	Properties
Use machine certificates	
	OK Cancel

步驟11.選擇OK並導航到C:\Windows\System32\drivers\etc。使用文本編輯器開啟hosts檔案。配置 條目以將網路連線中配置的(完全限定域名)FQDN解析為ASA頭端(在本例中為外部介面)的 IP地址。

#	For	example:			
#					
#		102.54.94.97	rhino.acme.com	#	source server
#		38.25.63.10	x.acme.com	#	x client host
1(.88.	.243.108 HeadEnd.d	avid.com		

步驟12.返回**控制面板>網路和Internet >網路連線**。選擇您建立的網路連線。按一下右鍵該連結,然 後選擇**「連線」。**

RA VPN to ASA with IKEv2		VirtualBox Host-Only		
Disconnected		Connect		
VMware Network Adapter Disabled VMware Virtual Ethernet A		Status		
		Set as Default Connection		
		Create Copy		
		Create Shortcut		
	۲	Delete		
	۲	Rename		
	•	Properties		

步驟13.網路連線狀態從「已斷開連線」轉變為「已連線」,然後轉變為「已連線」。最後,顯示您 為網路連線指定的名稱。



此時電腦已連線到VPN頭端。

配置Android本地VPN客戶端

步驟1.導覽至Settings>More connection Settings



步驟2.選擇VPN

A 🖬 🗄 🗄 🖬 🛓

🛛 🖀 🖬 54% 🛢 7:45 PN

More connection settings

Nearby device scanning

On

Printing

Download booster

VPN

Set up and manage Virtual Private Networks (VPNs).

步驟3.選擇Add VPN。如果連線已建立如本例所示,請輕觸引擎圖示以對其進行編輯。在「類型」 字段中指定IPSec IKEv2 RSA。Server address是啟用IKEv2的ASA介面IP地址。對於IPSec使用者 證書和IPSec CA證書,請點選下拉選單選擇安裝的證書。使用預設選項「從伺服器接收」保留 IPSec伺服器證書。





步驟4.選擇Save,然後點選新VPN連線的名稱。



步驟5.選擇**連線。**





步驟6.再次鍵入VPN連線以驗證狀態。現在顯示為Connected。





ASA頭端上的驗證命令:

ASA#show vpn-sessiondb detail ra-ikev2-ipsec Session Type: Generic Remote-Access IKEv2 IPsec Detailed Username : Win7_PC.david.com Index : 24 Assigned IP : 192.168.50.1 Public IP : 10.152.206.175 Protocol : IKEv2 IPsec License : AnyConnect Premium Encryption : IKEv2: (1)AES256 IPsec: (1)AES256 Hashing : IKEv2: (1)SHA1 IPsec: (1)SHA1 Bytes Tx : 0 Bytes Rx Bytes Rx : 16770 Pkts Tx : 0 Pkts Rx : 241 Pkts Tx Drop : 0 Pkts Rx Drop : 0 Group Policy : GP_David Tunnel Group : David Login Time : 08:00:01 UTC Tue Jul 18 2017 : 0h:00m:21s Duration Inactivity : 0h:00m:00s VLAN Mapping : N/A VLAN : none Audt Sess ID : 0a0a0a0100018000596dc001 Security Grp : none IKEv2 Tunnels: 1 IPsec Tunnels: 1 IKEv2: Tunnel ID : 24.1

UDP Src Port : 4500 UDP Dst Port : 4500 Rem Auth Mode: rsaCertificate Loc Auth Mode: rsaCertificate Encryption : AES256 Hashing : SHA1 Rekey Int (T): 86400 Seconds Rekey Left(T): 86379 Seconds PRF : SHA1 D/H Group : 2 Filter Name : TPsec: : 24.2 Tunnel ID Local Addr : 0.0.0.0/0.0.0/0/0 Remote Addr : 192.168.50.1/255.255.255.255/0/0 Encryption : AES256 Hashing : SHA1 Encapsulation: Tunnel Rekey Left(T): 28778 Seconds Rekey Int (T): 28800 Seconds Idle Time Out: 30 Minutes Idle TO Left : 30 Minutes Conn Time Out: 518729 Minutes Conn TO Left : 518728 Minutes Bytes Tx : 0 Bytes Rx : 16947 Pkts Tx : 0 Pkts Rx : 244 ASA# show crypto ikev2 sa IKEv2 SAs: Session-id:24, Status:UP-ACTIVE, IKE count:1, CHILD count:1 Remote Status Tunnel-id Local Role READY RESPONDER 2119549341 10.88.243.108/4500 10.152.206.175/4500 Encr: AES-CBC, keysize: 256, Hash: SHA96, DH Grp:2, Auth sign: RSA, Auth verify: RSA Life/Active Time: 86400/28 sec Child sa: local selector 0.0.0.0/0 - 255.255.255.255/65535 remote selector 192.168.50.1/0 - 192.168.50.1/65535 ESP spi in/out: 0xbfff64d7/0x76131476 ASA# show crypto ipsec sa interface: outside Crypto map tag: Anyconnect, seq num: 65535, local addr: 10.88.243.108 local ident (addr/mask/prot/port): (0.0.0.0/0.0.0/0/0) remote ident (addr/mask/prot/port): (192.168.50.1/255.255.255.255/0/0) current_peer: 10.152.206.175, username: Win7_PC.david.com dynamic allocated peer ip: 192.168.50.1 dynamic allocated peer ip(ipv6): 0.0.0.0 #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0 #pkts decaps: 339, #pkts decrypt: 339, #pkts verify: 339 #pkts compressed: 0, #pkts decompressed: 0 #pkts not compressed: 0, #pkts comp failed: 0, #pkts decomp failed: 0 #pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0 #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0 #TFC rcvd: 0, #TFC sent: 0 #Valid ICMP Errors rcvd: 0, #Invalid ICMP Errors rcvd: 0 #send errors: 0, #recv errors: 0 local crypto endpt.: 10.88.243.108/4500, remote crypto endpt.: 10.152.206.175/4500 path mtu 1496, ipsec overhead 58(44), media mtu 1500 PMTU time remaining (sec): 0, DF policy: copy-df ICMP error validation: disabled, TFC packets: disabled current outbound spi: 76131476 current inbound spi : BFFF64D7 inbound esp sas: spi: 0xBFFF64D7 (3221185751) transform: esp-aes-256 esp-sha-hmac no compression in use settings ={RA, Tunnel, IKEv2, } slot: 0, conn_id: 98304, crypto-map: Anyconnect sa timing: remaining key lifetime (sec): 28767 IV size: 16 bytes replay detection support: Y Anti replay bitmap: Oxffffffff Oxfffffff

outbound esp sas:									
spi: 0x76131476 (1980961910)	-						
transform: esp	-aes-256 e	sp-sha-	hmac :	no comp	pression	n			
in use setting	s ={RA, Tu	nnel, 1	KEV2,	}					
siou, o, conn_ia, 98304, crypto-map, Anyconnect sa timing: remaining key lifetime (sec): 28767									
TV size: 16 by	tes	TILCUL		CC)• 20	5707				
replay detecti	on support	: Y							
Anti replay bi	tmap:	_							
0x000000000	00000001								
ASA#show vpn-sessiondb	license-su	mmary							
VPN Licenses and Config	Jured Limit	s Summa							
							· · · · · · · · · · · · · · · · · · ·		
AnyConnect Premium		: ENAB	LED :		50 :	50	: NONE		
AnyConnect Essentials		: DISAB	LED :		50 :	0	: NONE		
Other VPN (Available by	r Default)	: ENAB	LED :		10 :	10	: NONE		
Shared License Server		: DISAB	LED						
Shared License Particip	pant	: DISAB	LED						
AnyConnect for Mobile		: ENAB	LED (R	equires	s Premi	um or Esse	entials)		
Advanced Endpoint Asses	sment	: ENAB	LED(R	equires	s Premi	um)			
AnyConnect for Cisco VE	N Phone	: ENAB	LED						
VPN-3DES-AES		: ENAB	LED						
VPN-DES		: ENAB	LED						
VPN Licenses Usage Summ	arv								
	Local :	Shared	.:	All :	Peak	: Eff.	:		
	In Use :	In Use	: In	Use :	In Use	: Limit	: Usage		
AnyConnect Premium	: 1:	0	:	1 :	1	: 50	: 2%		
AnyConnect Client	:		:	0 :	1		: 0%		
AnyConnect Mobile	:		:	0 :	0		: 0%		
Clientless VPN	:		:	0 :	0		: 0%		
Generic IKEv2 Client	:		:	1:	1		: 2%		
Other VPN	:		:	0 :	0	: 10	: 0%		
Cisco VPN Client	:		:	0 :	0		: 0%		
L2TP Clients									
Site-to-Site VPN	:		:	0 :	0		: 0%		
ASA# show won-sessiond	·								
	, 								
VPN Session Summary									
	Ac	tive :	Cumul	ative	Peak	Concur : :	Inactive		
American cit cit									
Anyconnect Client	•	0:		11	•	1.	U		
SSL/TLS/DTLS	:	0 :		1.0		1 :	0		
IKEV2 IPsec	:	0 :		10		1 :	0		
Generic IKEv2 Remote Ac	cess :	1:		14 :	:	1			
Total Active and Inacti	ve :	1		 To	otal Cu	mulative	: 25		
Device Total VPN Capaci	ty :	50							
Device Load	:	2%							
Tunnels Summarv									
		·							
	Ac	tive :	Cumul	ative	Peak (Concurrent	t		

IKEv2	:	1	:	: 25	:	1
IPsec	:	1	:	: 14	:	1
IPsecOverNatT	:	0	:	: 11	:	1
AnyConnect-Parent	:	0	:	: 11	:	1
SSL-Tunnel	:	0	:	: 1	:	1
DTLS-Tunnel	:	0	:	: 1	:	1
Totals	:	2	:	: 63		

疑難排解

本節提供的資訊可用於對組態進行疑難排解。

附註:使用debug指令之前,請先參閱<u>有關Debug</u>指令的重要資訊。

注意:在ASA上,您可以設定各種調試級別;預設情況下,使用級別1。如果更改調試級別,調 試的詳細程度會增加。請謹慎執行此操作,尤其是在生產環境中。

- Debug crypto ikev2 protocol 15
- Debug crypto ikev2 platform 15
- Debug crypto ca 255